AWS Cloud Data Protection Project – Implementation Guide

# 📘 Project Overview

This project focuses on protecting sensitive data (PII/PHI) stored in Amazon S3 by leveraging AWS-native services. It includes encryption using AWS KMS, automated classification with Amazon Macie, and real-time alerting using EventBridge and SNS. All findings are stored securely for long-term retention and audit purposes.

# 📐 Architecture Overview

1. Sensitive files are uploaded to an encrypted S3 bucket.  
2. AWS KMS is used to encrypt objects using SSE-KMS.  
3. Amazon Macie scans the bucket using classification jobs.  
4. Macie findings are exported to a second S3 bucket.  
5. EventBridge routes findings to an SNS topic.  
6. SNS sends an email alert to subscribed users.

# 🛠️ Implementation Steps

1. Create an S3 bucket named `org-sensitive-data-yourname` for storing sensitive files.

2. Enable SSE-KMS encryption using a Customer Managed Key (CMK).

3. Create a second bucket named `macie-discovery-results-yourname` to store Macie results.

4. Create a CMK in AWS KMS with permissions for Macie and your IAM user.

5. Apply the correct bucket policy to both S3 buckets to allow Macie access.

6. Configure the KMS key policy to allow Macie (`arn:aws:iam::112758395563:root`) to encrypt/decrypt.

7. Enable Amazon Macie in the same region as your S3 buckets.

8. Upload sample PII/PHI test files (≥1 KB) to the data bucket.

9. Create a Macie classification job with managed data identifiers.

10. Create an SNS topic and subscribe your email to receive alerts.

11. Create an EventBridge rule to capture Macie findings and forward to SNS.

12. Re-run the Macie classification job and confirm that findings appear, are exported to the discovery bucket, and alerts are received.

# 🧪 Testing & Validation

After configuring all services and policies:  
- Upload new test files to the S3 bucket  
- Run a Macie job and ensure findings are generated  
- Confirm finding exports in the results bucket  
- Verify email alert is triggered via SNS